

1 Frank S. Hedin (SBN 291289)  
2 Hedin LLP  
3 535 Mission Street, 14th Floor  
4 San Francisco, CA 94105  
5 Telephone: (305) 357-2107  
6 Facsimile: (305) 200-8801  
7 E-Mail: fhedin@hedinllp.com

8 *Attorney for Plaintiffs and the Putative Classes*

9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA**

ALAN SILVA and ELIZABETH MALATY-  
UHR, individually and on behalf of all others  
similarly situated,

Plaintiffs,

v.

YANKA INDUSTRIES, INC. D/B/A  
MASTERCLASS,

Defendant.

Case No. 3:24-cv-05264-PHK

**SECOND AMENDED CLASS  
ACTION COMPLAINT**

**DEMAND FOR JURY TRIAL**

Alan Silva (“Plaintiff Silva”) and Elizabeth Malaty-Uhr (“Plaintiff Malaty-Uhr”), individually and on behalf of all others similarly situated, make the following allegations pursuant to the investigation of counsel and based upon information and belief, except as to allegations pertaining specifically to themselves or their counsel, which are based on personal knowledge.

**NATURE OF THE CASE**

1. Plaintiffs bring this action for legal and equitable remedies to redress and put a stop to Defendant Yanka Industries Inc. d/b/a MasterClass’s practices of knowingly selling, transmitting, and/or otherwise disclosing, to various third parties,

1 records containing the personal information of each of their subscribers, along with the  
2 detailed information revealing their purchase of a subscription to Defendant's video  
3 service (collectively "Personal Viewing Information") in violation of the Video Privacy  
4 Protection Act, 18 U.S.C. §2710 et seq. ("VPPA").  
5

6         2. Over the past two years, Defendant has systematically transmitted (and  
7 continues to transmit today) its subscribers' personally identifying video subscription  
8 purchase information to Meta using a snippet of programming code called the "Meta  
9 Pixel," which Defendant chose to install on its masterclass.com website. Defendant also  
10 systematically transmitted (and continues to transmit today) its subscribers' personally  
11 identifying video viewing information to Google Analytics ("Google"), another tracker  
12 that Defendant chose to install on its website.  
13

14         3. The information Defendant disclosed (and continues to disclose) to Meta,  
15 via the Meta Pixel it installed on its website, includes the subscriber's Facebook ID  
16 ("FID") coupled with the fact that the subscriber requested or obtained a subscription to  
17 the videos available exclusively on Defendant's website. A subscriber's FID is a unique  
18 sequence of numbers linked to the Meta profile belonging to that subscriber. The  
19 subscriber's Meta profile, in turn, publicly identifies the subscriber by name (and  
20 contains other personally identifying information about the subscriber as well).  
21 Entering "facebook.com/[FID]" into a web browser returns the Meta profile of the person  
22 to whom the FID corresponds. Thus, the FID identifies a person more precisely than a  
23 name, as numerous persons may share the same name but each person's Facebook  
24 profile (and associated FID) uniquely identifies one and only one person. In the simplest  
25 terms, the Meta Pixel installed by Defendant captures and discloses to Meta information  
26  
27  
28

1 that reveals that a particular person purchased a subscription to Defendant's website  
2 (hereinafter, "Private Viewing Information").

3 4. The information Defendant disclosed (and continues to disclose) to Google  
4 Analytics via the Google Tag Manager it installed on its website includes the specific  
5 video title and unique user data sufficient for Google Analytics to identify the subscriber.  
6

7 5. Defendant disclosed and continues to disclose its subscribers' Private  
8 Viewing Information to Meta and Google without asking for let alone obtaining its  
9 subscribers' consent to these practices.  
10

11 6. The VPPA clearly prohibits what Defendant has done. Subsection (b)(1) of  
12 the VPPA provides that, absent the consumer's prior informed, written consent, any  
13 "video tape service provider who knowingly discloses, to any person, personally  
14 identifiable information concerning any consumer of such provider shall be liable to the  
15 aggrieved person for," 18 U.S.C. § 2710(b)(1), *inter alia*, liquidated damages in the  
16 amount of \$2,500.00 per violation and equitable relief, *see id.* § 2710(c).  
17

18 7. Accordingly, on behalf of themselves and members of the Classes defined  
19 below, Plaintiffs bring this Second Amended Class Action Complaint against  
20 Defendant for intentionally and unlawfully disclosing their Personal Viewing  
21 Information to Meta and Google.<sup>1</sup>  
22  
23  
24  
25  
26

---

27 <sup>1</sup> This Second Amended Class Action Complaint is filed with permission from opposing  
28 counsel pursuant to Federal Rule of Civil Procedure 15(a)(2).

**PARTIES**

**I. Plaintiff Silva**

8. Plaintiff Silva is, and at all times relevant hereto was, a citizen and resident of Bedford County in Alum Bank, Pennsylvania.

9. Plaintiff Silva is, and at all times relevant hereto was, a user of Meta.

10. Plaintiff Silva is a consumer of the video products and services offered on Defendant's masterclass.com website. He first subscribed to Defendant's website in or about December 2023 and has continuously maintained his subscription since then. Plaintiff Silva became a subscriber to Defendant's website by registering and paying for a subscription via the Google quick sign-up feature, which automatically pulled over his name, email address, payment information, and zip code from his Google account.

11. On multiple occasions during the two years preceding the filing of this action, Plaintiff Silva used his subscription to Defendant's website to request and obtain pre-recorded videos from Defendant. On each such occasion, Defendant disclosed to Google the specific title of the video he requested and obtained and the URL where he requested access to and obtained the video coupled with information sufficient for Google to identify Plaintiff Silva, including his personal IP Address, among other information concerning Plaintiff Silva and the device on which he used to request and obtain the video.

12. At all times relevant hereto, including when purchasing a subscription to Defendant's website and accessing and obtaining the prerecorded video material provided to subscribers on Defendant's website, Plaintiff Silva had a Meta account, a

1 Meta profile, and an FID associated with such profile.

2 13. Plaintiff Silva has never consented, agreed, authorized, or otherwise  
3 permitted Defendant to disclose his Personal Viewing Information to Meta or Google.  
4 In fact, Defendant has never even provided Plaintiff Silva with written notice of its  
5 practices of disclosing its customers' Personal Viewing Information to third parties such  
6 as Meta or Google.  
7

8 14. Because Defendant disclosed Plaintiff Silva's Private Viewing Information  
9 (including his FID and his purchase of a subscription to Defendant's website) to Meta  
10 and his Private Viewing Information to Google during the applicable statutory period,  
11 Defendant violated Plaintiff Silva's rights under the VPPA and invaded his statutorily  
12 conferred interest in keeping such information (which bears on his personal affairs and  
13 concerns) private.  
14

15 **II. Plaintiff Malaty-Uhr**  
16

17 15. Plaintiff Malaty-Uhr is, and at all times relevant hereto was, a citizen and  
18 resident of DuPage County, Illinois.

19 16. Plaintiff Malaty-Uhr is, and at all times relevant hereto was, a user of  
20 Meta.  
21

22 17. Plaintiff Malaty-Uhr is a consumer of the video products and services  
23 offered on Defendant's masterclass.com website. She first subscribed to Defendant's  
24 website on or about December 2023 and has continuously maintained her subscription  
25 since then. Plaintiff Malaty-Uhr became a subscriber to Defendant's website by  
26 registering and paying for a subscription via the Google quick sign-up feature, which  
27  
28

1 automatically pulled over her name, email address, payment information, and zip code  
2 from her Google account.

3       18. On multiple occasions during the two years preceding the filing of this  
4 action, Plaintiff Malaty-Uhr used her subscription to Defendant's website to request  
5 and obtain pre-recorded videos from Defendant. On each such occasion, Defendant  
6 disclosed to Google the specific title of the video she requested and obtained and the  
7 URL where she requested access to and obtained the video coupled with information  
8 sufficient for Google to identify Plaintiff Malaty-Uhr, including her personal IP  
9 address, among other information concerning Plaintiff Malaty-Uhr and the device on  
10 which she used to request and obtain the video.  
11

12  
13       19. At all times relevant hereto, including when purchasing a subscription to  
14 Defendant's website and accessing and obtaining the prerecorded video material  
15 provided to subscribers on Defendant's website, Plaintiff Malaty-Uhr had a Meta  
16 account, a Meta profile, and an FID associated with such profile.  
17

18       20. Plaintiff Malaty-Uhr has never consented, agreed, authorized, or otherwise  
19 permitted Defendant to disclose her Personal Viewing Information to Meta or Google.  
20 In fact, Defendant has never even provided Plaintiff Malaty-Uhr with written notice of  
21 its practices of disclosing its customers' Personal Viewing Information to third parties  
22 such as Meta or Google.  
23

24       21. Because Defendant disclosed Plaintiff Malaty-Uhr's Private Viewing  
25 Information (including her FID and her purchase of a subscription to Defendant's  
26 website) to Meta and her Private Viewing Information to Google during the applicable  
27 statutory period, Defendant violated Plaintiff Malaty-Uhr's rights under the VPPA and  
28

1 invaded her statutorily conferred interest in keeping such information (which bears on  
2 her personal affairs and concerns) private.

3  
22. **Defendant Yanka Industries Inc. d/b/a MasterClass**

4  
5 23. Defendant is a Delaware Foreign Business Corporation with its  
6 headquarters and principal place of business located at 660 4th Street, San Francisco,  
7 CA 94107.

8  
9 24. Defendant operates and maintains the website masterclass.com, where it  
10 sells subscriptions to consumers to access prerecorded video content and provides its  
11 subscribers with access to a digital library comprised of various types of pre-recorded  
12 instructional and educational videos.

13 **JURISDICTION AND VENUE**

14 25. This Court has subject-matter jurisdiction over this civil action pursuant  
15 to 28 U.S.C. § 1331 and 18 U.S.C. § 2710.

16  
17 26. Personal jurisdiction and venue are proper because Defendant maintains  
18 its headquarters and principal place of business in San Francisco, CA, within this  
19 judicial District.

20 **VIDEO PRIVACY PROTECTION ACT**

21  
22 27. Generally speaking, the VPPA prohibits companies like Defendant from  
23 knowingly disclosing to third parties like Facebook information that personally  
24 identifies consumers like Plaintiffs as having viewed particular videos or other audio-  
25 visual products or services.

26  
27 28. Specifically, subject to certain exceptions that do not apply here, the VPPA  
28 prohibits “a video tape service provider” from “knowingly disclos[ing], to any person,

1 personally identifiable information concerning any consumer of such provider[.]” 18  
2 U.S.C. § 2710(b)(1). The statute defines a “video tape service provider” as “any person,  
3 engaged in the business...of rental, sale, or delivery of prerecorded video cassette tapes  
4 or similar audio visual materials,” 18 U.S.C. § 2710(a)(4), and defines a “consumer” as  
5 “a renter, purchaser, or subscriber of goods or services from a video tape service  
6 provider.” 18 U.S.C. § 2710(a)(1). “[P]ersonally identifiable information’ includes  
7 information which identifies a person as having requested or obtained specific video  
8 materials or services from a video tape service provider.” 18 U.S.C. § 2710(a)(3)  
9

10  
11 29. The VPPA’s purpose is as apropos today as it was at the time of its  
12 enactment over 35 years ago. Leading up to the statute’s enactment in 1988, members  
13 of the United States Senate warned that “[e]very day Americans are forced to provide  
14 to businesses and others personal information without having any control over where  
15 that information goes.” *Id.* Senators at the time were particularly troubled by  
16 disclosures of records that reveal consumers’ purchases and rentals of videos and other  
17 audiovisual materials, because such records offer “a window into our loves, likes, and  
18 dislikes,” such that “the trail of information generated by every transaction that is now  
19 recorded and stored in sophisticated record-keeping systems is a new, more subtle and  
20 pervasive form of surveillance.” S. Rep. No. 100-599 at 7-8 (1988) (statements of Sens.  
21 Simon and Leahy, respectively).  
22  
23

24 30. Thus, in proposing the Video and Library Privacy Protection Act (which  
25 later became the VPPA), Senator Patrick J. Leahy (the senior Senator from Vermont  
26 from 1975 to 2023) sought to codify, as a matter of law, that “our right to privacy protects  
27 the choice of movies that we watch with our family in our own homes.” 134 Cong. Rec.  
28



1 S5399 (May 10, 1988). As Senator Leahy explained at the time, it is the personal nature  
 2 of such information, and the need to protect it from disclosure, that is the *raison d'être*  
 3 of the statute: “These activities are at the core of any definition of personhood. They  
 4 reveal our likes and dislikes, our interests and our whims. They say a great deal about  
 5 our dreams and ambitions, our fears and our hopes. They reflect our individuality, and  
 6 they describe us as people.” *Id.*

8 31. While these statements rang true in 1988 when the act was passed, the  
 9 importance of legislation like the VPPA in the modern era of data mining is more  
 10 pronounced than ever before. During a recent Senate Judiciary Committee meeting,  
 11 “The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century,”  
 12 Senator Leahy emphasized the point by stating: “While it is true that technology has  
 13 changed over the years, we must stay faithful to our fundamental right to privacy and  
 14 freedom. Today, social networking, video streaming, the ‘cloud,’ mobile apps and other  
 15 new technologies have revolutionized the availability of Americans’ information.”<sup>2</sup>

18 32. Former Senator Al Franken may have said it best: “If someone wants to  
 19 share what they watch, I want them to be able to do so . . . But I want to make sure that  
 20 consumers have the right to easily control who finds out what they watch—and who  
 21 doesn’t. The Video Privacy Protection Act guarantees them that right.”<sup>3</sup>

---

23 <sup>2</sup> The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century,  
 24 Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law,  
 25 <http://www.judiciary.senate.gov/meetings/the-video-privacy-protection-act-protecting-viewer-privacy-in-the-21stcentury>.

26 <sup>3</sup> Chairman Franken Holds Hearing on Updated Video Privacy Law for 21st  
 27 Century,  
 28 [frank.senate.gov](http://frank.senate.gov) (Jan. 31, 2012).

33. In this case, however, Defendant deprived Plaintiffs and the unnamed Class members of that right by systematically (and surreptitiously) disclosing their Personal Viewing Information to Facebook, without providing notice to (let alone obtaining consent from) any of them, as explained in detail below.

## BACKGROUND FACTS

### I. Consumers' Personal Information Has Real Market Value

34. In 2001, Federal Trade Commission ("FTC") Commissioner Orson Swindle remarked that "the digital revolution . . . has given an enormous capacity to the acts of collecting and transmitting and flowing of information, unlike anything we've ever seen in our lifetimes . . . [and] individuals are concerned about being defined by the existing data on themselves."<sup>4</sup>

35. More than a decade later, Commissioner Swindle's comments ring truer than ever, as consumer data feeds an information marketplace that supports a \$26 billion dollar per year online advertising industry in the United States.<sup>5</sup>

36. The FTC has also recognized that consumer data possesses inherent monetary value within the new information marketplace and publicly stated that:

Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency.

---

<sup>4</sup> FCC, *The Information Marketplace* (Mar. 13, 2001), at 8-11, available at [https://www.ftc.gov/sites/default/files/documents/public\\_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf](https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf).

<sup>5</sup> See *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011), <http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html>.

1           The larger the data set, the greater potential for analysis –  
2           and profit.<sup>6</sup>

3           37. In fact, an entire industry exists while companies known as data  
4 aggregators purchase, trade, and collect massive databases of information about  
5 consumers. Data aggregators then profit by selling this “extraordinarily intrusive”  
6 information in an open and largely unregulated market.<sup>7</sup>

7  
8           38. The scope of data aggregators’ knowledge about consumers is immense: “If  
9 you are an American adult, the odds are that [they] know[] things like your age, race,  
10 sex, weight, height, marital status, education level, politics, buying habits, household  
11 health worries, vacation dreams—and on and on.”<sup>8</sup>

12  
13           39. Further, “[a]s use of the Internet has grown, the data broker industry has  
14 already evolved to take advantage of the increasingly specific pieces of information  
15 about consumers that are now available.”<sup>9</sup>

16           40. Recognizing the serious threat the data mining industry poses to  
17 consumers’ privacy, on July 25, 2012, the co-Chairmen of the Congressional Bi-Partisan  
18

19           <sup>6</sup> Statement of FTC Cmr. Harbour (Dec. 7, 2009), at 2, *available at*  
20 [https://www.ftc.gov/sites/default/files/documents/public\\_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf](https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf).

21           <sup>7</sup> See M. White, *Big Data Knows What You’re Doing Right Now*, TIME.com (July  
22 31, 2012), <http://moneyland.time.com/2012/07/31/big-data-knows-what-youre-doing-right-now/>.

23           <sup>8</sup> N. Singer, *You for Sale: Mapping, and Sharing, the Consumer Genome*, N.Y.  
24 Times (June 16, 2012), *available at*  
25 <http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html>.

26           <sup>9</sup> Letter from Sen. J. Rockefeller IV, Sen. Cmtee. on Commerce, Science, and  
27 Transportation, to S. Howe, Chief Executive Officer, Acxiom (Oct. 9, 2012) *available at*  
28 [http://www.commerce.senate.gov/public/?a=Files.Serve&File\\_id=3bb94703-5ac8-4157-a97b-a658c3c3061c](http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=3bb94703-5ac8-4157-a97b-a658c3c3061c).

1 Privacy Caucus sent a letter to nine major data brokerage companies seeking  
2 information on how those companies collect, store, and sell their massive collections of  
3 consumer data, stating in pertinent part:

4  
5 By combining data from numerous offline and online sources,  
6 data brokers have developed hidden dossiers on every U.S.  
7 consumer. This large[-]scale aggregation of the personal  
information of hundreds of millions of American citizens  
raises a number of serious privacy concerns.<sup>10</sup>

8 41. Data aggregation is especially troublesome when consumer information is  
9 sold to direct-mail advertisers. In addition to causing waste and inconvenience, direct-  
10 mail advertisers often use consumer information to lure unsuspecting consumers into  
11 various scams, including fraudulent sweepstakes, charities, and buying clubs. Thus,  
12 when companies like Defendant share information with data aggregators, data  
13 cooperatives, and direct-mail advertisers, they contribute to the “[v]ast databases” of  
14 consumer data that are often “sold to thieves by large publicly traded companies,” which  
15 “put[s] almost anyone within the reach of fraudulent telemarketers” and other  
16 criminals.<sup>11</sup>

17  
18  
19 42. Disclosures like Defendant’s are particularly dangerous to the elderly.  
20 “Older Americans are perfect telemarketing customers, analysts say, because they are  
21 often at home, rely on delivery services, and are lonely for the companionship that  
22  
23

24  
25 <sup>10</sup> See *Bipartisan Group of Lawmakers Query Data Brokers About Practices*  
26 *Involving Consumers’ Personal Information*, Website of Sen. Markey (July 24, 2012),  
[http://www.markey.senate.gov/news/press-releases/bipartisan-group-of-lawmakers-](http://www.markey.senate.gov/news/press-releases/bipartisan-group-of-lawmakers-query-data-brokers-about-practices-involving-consumers-personal-information)  
[query-data-brokers-about-practices-involving-consumers-personal-information](http://www.markey.senate.gov/news/press-releases/bipartisan-group-of-lawmakers-query-data-brokers-about-practices-involving-consumers-personal-information).

27 <sup>11</sup> See Charles Duhigg, *Bilking the Elderly, with a Corporate Assist*, N.Y. Times (May 20, 2007),  
available at <https://www.nytimes.com/2007/05/20/business/20tele.html>.

1 telephone callers provide.”<sup>12</sup> The FTC notes that “[t]he elderly often are the deliberate  
 2 targets of fraudulent telemarketers who take advantage of the fact that many older  
 3 people have cash reserves or other assets to spend on seemingly attractive offers.”<sup>13</sup>  
 4

5 43. Indeed, an entire black market exists while the personal information of  
 6 vulnerable elderly Americans is exchanged. Thus, information disclosures like  
 7 Defendant’s are particularly troublesome because of their cascading nature: “Once  
 8 marked as receptive to [a specific] type of spam, a consumer is often bombarded with  
 9 similar fraudulent offers from a host of scam artists.”<sup>14</sup>  
 10

11 44. Defendant is not alone in violating its customers’ statutory rights and  
 12 jeopardizing their well-being in exchange for increased revenue: disclosing customer  
 13 and subscriber information to data aggregators, data appenders, data cooperatives,  
 14 direct marketers, and other third parties has become a widespread practice.  
 15 Unfortunately for consumers, however, this growth has come at the expense of their  
 16 most basic privacy rights.  
 17

## 18 **II. Consumers Place Monetary Value on their Privacy and Consider** 19 **Privacy Practices When Making Purchases**

20 45. As the data aggregation industry has grown, so too have consumer  
 21 concerns regarding their personal information.  
 22  
 23

---

24 <sup>12</sup> *Id.*

25 <sup>13</sup> *Fraud Against Seniors: Hearing before the Senate Special Committee on Aging*  
 26 (August 10, 2000) (prepared statement of the FTC), *available at*  
 27 [https://www.ftc.gov/sites/default/files/documents/public\\_statements/prepared-](https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-fraud-against-seniors/agingtestimony.pdf)  
 28 [statement-federal-trade-commission-fraud-against-seniors/agingtestimony.pdf](https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-fraud-against-seniors/agingtestimony.pdf).

<sup>14</sup> *Id.*

1        46. A recent survey conducted by Harris Interactive on behalf of TRUSTe, Inc.  
2 showed that 89 percent of consumers polled avoid doing business with companies who  
3 they believe do not protect their privacy online.<sup>15</sup> As a result, 81 percent of smartphone  
4 users polled said that they avoid using smartphone apps that they don't believe protect  
5 their privacy online.<sup>16</sup>  
6

7        47. Thus, as consumer privacy concerns grow, consumers are increasingly  
8 incorporating privacy concerns and values into their purchasing decisions and  
9 companies viewed as having weaker privacy protections are forced to offer greater value  
10 elsewhere (through better quality and/or lower prices) than their privacy- protective  
11 competitors.  
12

13        48. In fact, consumers' personal information has become such a valuable  
14 commodity that companies are beginning to offer individuals the opportunity to sell  
15 their personal information themselves.<sup>17</sup>  
16

17        49. These companies' business models capitalize on a fundamental tenet  
18 underlying the personal information marketplace: consumers recognize the economic  
19 value of their private data. Research shows that consumers are willing to pay a  
20  
21  
22

---

23 <sup>15</sup> See 2014 TRUSTe US Consumer Confidence Privacy Report, TRUSTe,  
24 [http://www.theagitator.net/wp-content/uploads/012714\\_ConsumerConfidenceReport\\_US1.pdf](http://www.theagitator.net/wp-content/uploads/012714_ConsumerConfidenceReport_US1.pdf).

25 <sup>16</sup> *Id.*

26 <sup>17</sup> See Joshua Brustein, *Start-Ups Seek to Help Users Put a Price on Their Personal*  
27 *Data*, N.Y. Times (Feb. 12, 2012), available at  
28 <http://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html>.

1 premium to purchase services from companies that adhere to more stringent policies of  
2 protecting their personal data.<sup>18</sup>

3  
4 50. Thus, in today's digital economy, individuals and businesses alike place a  
5 real, quantifiable value on consumer data and corresponding privacy rights.<sup>19</sup> As such,  
6 where a business offers customers a service that includes statutorily guaranteed privacy  
7 protections, yet fails to honor these guarantees, the customer receives a service of less  
8 value than the service paid for.

### 9 **III. Defendant Systematically Discloses its Subscribers' Personal** 10 **Viewing Information to Meta**

11 51. As alleged below, when a consumer requests or obtains a specific  
12 subscription to Defendant's website, the Meta Pixel technology that Defendant  
13 intentionally installed on its website transmits the fact that a consumer purchased a  
14 subscription to video services alongside his or her FID to Meta, without the subscriber's  
15 consent and in clear violation of the VPPA.

17 52. Also, when a subscriber to Defendant's website requests or obtains a  
18 specific video, the Google technology that Defendant intentionally installed on its  
19 website transmits unique information sufficient for Google to identify the user and  
20

---

22 <sup>18</sup> See Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy*  
23 *Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254  
24 (2011); see also European Network and Information Security Agency, *Study on*  
25 *monetising privacy* (Feb. 27, 2012), available at  
<https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy>.

26 <sup>19</sup> See Hann, et al., *The Value of Online Information Privacy: An Empirical*  
27 *Investigation* (Oct. 2003) at 2, available at  
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.321.6125&rep=rep1&type=pdf>  
28 f ("It is obvious that people value online privacy.").

1 detailed information concerning the specific interactions the subscriber takes on its  
2 website (including the subscriber's Private Viewing Information revealing the specific  
3 videos that he or she requested) to Google, without the subscriber's consent and in clear  
4 violation of the VPPA.  
5

#### 6 **A. The Meta Pixel**

7 53. On February 4, 2004, Mark Zuckerberg and others launched Facebook,  
8 now known as "Meta".<sup>20</sup> Since then, Meta has become the world's largest social media  
9 platform. To create a Meta account, a person must provide, *inter alia*, his or her first  
10 and last name, birthdate, gender, and phone number or email.  
11

12 54. The Meta Pixel, first introduced in 2013 as the "Facebook Pixel," is a  
13 unique string of code that companies can embed on their websites to allow them to track  
14 consumers' actions and report the actions back to Meta.  
15

16 55. The Meta Pixel allows online-based companies like Defendant to build  
17 detailed profiles about their visitors by collecting information about how they interact  
18 with their websites, and to then use the collected information to service highly targeted  
19 advertising to them.  
20

21 56. Additionally, a Meta Pixel installed on a company's website allows Meta  
22 "to match . . . website visitors to their respective [Meta] User accounts."<sup>21</sup> Meta is able  
23 to do this because it has assigned to each of its users an "FID" number – a unique and  
24 persistent identifier that allows anyone to look up the user's unique Meta profile and  
25

---

26 <sup>20</sup> Company Info, FACEBOOK, <https://about.fb.com/company-info/>.

27 <sup>21</sup> <https://developers.facebook.com/docs/meta-pixel/get-started>.  
28



1 thus identify the user by name<sup>22</sup> – and because each transmission of information made  
 2 from a company’s website to Meta via the Meta Pixel is accompanied by, *inter alia*, the  
 3 FID of the website’s visitor. Moreover, the Meta Pixel can follow a consumer to different  
 4 websites and across the Internet even after clearing browser history.  
 5

6 57. Meta has used the Meta Pixel to amass a vast digital database of dossiers  
 7 comprised of highly detailed personally identifying information about each of its billions  
 8 of users worldwide, including information about all of its users’ interactions with any of  
 9 the millions of websites across the Internet on which the Meta Pixel is installed. Meta  
 10 then monetizes this Orwellian database by selling advertisers the ability to serve highly  
 11 targeted advertisements to the persons whose personal information is contained within  
 12 it.  
 13

14 58. Simply put: if a company chooses to install the Meta Pixel on its website,  
 15 both the company who installed it and Meta (the recipient of the information it  
 16 transmits) are then able to “track[] the people and type of actions they take”<sup>23</sup> on the  
 17 company’s website, including the purchases they made, the items they spent time  
 18 viewing, and, as relevant here, the specific video content that they requested or obtained  
 19 on the website.  
 20

21 **B. Defendant Knowingly Uses the Meta Pixel to Transmit the Private**  
 22 **Viewing Information of all of its Subscribers to Meta**  
 23

24 \_\_\_\_\_  
 25 <sup>22</sup> For example, Mark Zuckerberg’s FID is reportedly the number “4,” so logging into  
 26 Facebook and typing [www.facebook.com/4](http://www.facebook.com/4) in the web browser retrieves Mark  
 27 Zuckerberg’s Facebook page: [www.facebook.com/zuck](http://www.facebook.com/zuck), and all of the additional  
 personally identifiable information contained therein.

28 <sup>23</sup> <https://www.facebook.com/business/goals/retargeting>.

1           59. Defendant allows persons to become digital consumers of its various  
2 online-based video products and services by subscribing to its website. To subscribe, the  
3 consumer must provide at least his or her name, email address, billing address, and  
4 credit- or debit-card (or other form of payment) information.  
5

6           60. When a person is completing the subscription process to gain access to  
7 videos on Defendant's website, Defendant uses – and has used at all times relevant  
8 hereto – the Meta Pixel to disclose to Meta the unencrypted FID of the subscriber and  
9 the fact that the person is requesting or obtaining a subscription to Defendant's website.  
10

11           61. Defendant intentionally programmed its website (by following step-by-  
12 step instructions from Meta's website) to include a Meta Pixel that systematically  
13 transmits to Meta the FIDs of its subscribers and the fact that a subscription was  
14 purchased by each of them in order to take advantage of the targeted advertising and  
15 other informational and analytical services offered by Meta.  
16

17           62. With only a person's FID and the knowledge that a person purchased a  
18 subscription to Defendant's website—all of which Defendant knowingly provides to  
19 Meta —any ordinary person could learn the identity of the person to whom the FID  
20 corresponds and the specific video products or services that this person requested. This  
21 can be accomplished simply by accessing the URL [www.facebook.com/\[unencrypted](http://www.facebook.com/[unencrypted FID])  
22 [FID\]](http://www.facebook.com/[unencrypted FID])/.  
23

24           63. Defendant's practices of disclosing that Plaintiffs and members of the  
25 Classes purchased subscriptions on Defendant's website to Meta continued unabated  
26 for the full duration of the time period relevant to this action. At all times relevant  
27 hereto, whenever Plaintiffs or another subscriber of Defendant's website requested or  
28

1 obtained a particular subscription (by clicking on it) on Defendant's website, Defendant  
2 disclosed to Meta that (*inter alia*) the purchaser requested or obtained a subscription to  
3 video services, along with the FID of the subscriber who requested it (which, as  
4 discussed above, uniquely identifies the person).  
5

6 64. At all relevant times, Defendant knew the Meta Pixel disclosed its  
7 subscribers' Private Viewing Information to Meta.

8 65. Defendant could easily have programmed its website so that none of its  
9 subscribers' detailed Private Viewing Information is disclosed to Meta. Instead,  
10 Defendant chose to program its website so that all of its subscribers' detailed Private  
11 Viewing Information is sent to Meta *en masse*.  
12

13 66. Google Analytics functions like the Meta Pixel, in that, when a subscriber  
14 to Defendant's website requests or obtains a specific video, Google Analytics – as  
15 intentionally installed on Defendant's website – transmits or collects unique  
16 information sufficient for Google to identify the user including by their IP Address and  
17 other detailed information concerning the specific interactions the subscriber takes on  
18 its website (including the subscriber's Private Viewing Information revealing the  
19 specific videos that he or she requested), without the subscriber's consent and in clear  
20 violation of the VPPA.  
21  
22

23 67. Prior to transmitting its subscribers' Private Viewing Information to Meta,  
24 Defendant failed to notify Plaintiffs or any of its other subscribers that it would do so,  
25 and neither Plaintiffs nor any of its other subscribers have consented (in writing or  
26 otherwise) to these practices.  
27

28 68. By intentionally disclosing to Meta Plaintiffs' and its other subscribers'

1 FIDs together with the specific video content they each requested or obtained, without  
 2 Plaintiffs' or any of its other subscribers' consent to these practices, Defendant  
 3 knowingly and systematically violated the VPPA on an enormous scale.

#### 4 **CLASS ACTION ALLEGATIONS**

6 69. Plaintiffs seek to represent two classes defined as follows:

7 **Meta Class:** All persons in the United States who, during the two  
 8 years preceding the filing of this action, requested or obtained a  
 9 subscription to Defendant's website while maintaining an account with  
 Meta Platforms, Inc. f/k/a Facebook, Inc.

10 **Google Class:** All persons in the United States who, during the two  
 11 years preceding the filing of this action, requested or obtained video  
 12 content as a subscriber of Defendant's website while maintaining an  
 account with Google.

13 70. Class members are so numerous that their individual joinder herein is  
 14 impracticable. On information and belief, members of the Classes number in at least  
 15 the tens of thousands. The precise number of Class members and their identities are  
 16 unknown to Plaintiffs at this time but may be determined through discovery. Members  
 17 of the Classes may be notified of the pendency of this action by mail and/or publication  
 18 through the membership records of Defendant.

20 71. Common questions of law and fact exist for members of all Classes and  
 21 predominate over questions affecting only individual class members. Common legal and  
 22 factual questions include, but are not limited to: (a) whether Defendant knowingly  
 23 disclosed Plaintiffs' and Class members' Private Viewing Information to Meta; (b)  
 24 whether Defendant's conduct violates the Video Privacy Protection Act, 18 U.S.C. §  
 25 2710; (c) whether Defendant should be enjoined from disclosing Plaintiffs' and Class  
 26 members' Private Viewing Information to Meta; (d) whether Defendant should be  
 27

1 enjoined from disclosing Plaintiffs' and Class members' Private Viewing Information to  
2 Google; and (e) whether Plaintiffs and Class members are entitled to statutory damages  
3 for the aforementioned violations.

4  
5 72. The named Plaintiffs' claims are typical of the claims of the Classes in that  
6 the named Plaintiffs and the Class members suffered invasions of their statutorily  
7 protected right to privacy (as afforded by the VPPA), as well as intrusions upon their  
8 private affairs and concerns that would be highly offensive to a reasonable person, as a  
9 result of Defendant's uniform and wrongful conduct in intentionally disclosing their  
10 Private Viewing Information to Meta and Google.

11  
12 73. Plaintiffs are adequate representatives of the Classes because their  
13 interests do not conflict with the interests of the Class members they seek to represent,  
14 they have retained competent counsel experienced in prosecuting class actions, and they  
15 intend to prosecute this action vigorously. Plaintiffs and their counsel will fairly and  
16 adequately protect the interests of members of the Classes.

17  
18 74. The class mechanism is superior to other available means for the fair and  
19 efficient adjudication of Classes claims. Each individual member of the Classes may  
20 lack the resources to undergo the burden and expense of individual prosecution of the  
21 complex and extensive litigation necessary to establish Defendant's liability.  
22 Individualized litigation increases the delay and expense to all parties and multiplies  
23 the burden on the judicial system presented by this case's complex legal and factual  
24 issues. Individualized litigation also presents a potential for inconsistent or  
25 contradictory judgments. In contrast, the class action device presents far fewer  
26 management difficulties and provides the benefits of single adjudication, economy of  
27

scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

## **CAUSES OF ACTION**

### **COUNT ONE**

#### **Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710**

##### **Meta Class**

75. Plaintiffs repeat the allegations from paragraphs (1-51, 53-65, 67-74) as if fully set forth herein.

76. Plaintiffs bring this claim individually and on behalf of the Meta Class Members against Defendant.

77. The VPPA prohibits a "video tape service provider" from knowingly disclosing "personally identifying information" concerning any "consumer" to a third party without the "informed, written consent (including through an electronic means using the Internet) of the consumer." 18 U.S.C. § 2710.

78. As defined in 18 U.S.C. § 2710(a)(4), a "video tape service provider" is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials[.]" Defendant is a "video tape service provider" as defined in 18 U.S.C. § 2710(a)(4) because it is engaged in the business of delivering audiovisual materials that are similar to prerecorded video cassette tapes and those sales affect interstate or foreign commerce.

79. As defined in 18 U.S.C. § 2710(a)(1), a "consumer" means any renter, purchaser, or consumer of goods or services from a video tape service provider." As alleged above, Plaintiffs and the Meta Class members are consumers because they

1 purchased a subscription to prerecorded video content on Defendant's website. Thus,  
2 Plaintiffs and the Meta Class members are "consumers" as defined in 18 U.S.C. §  
3 2710(a)(1).  
4

5 80. As defined in 18 U.S.C. § 2710(a)(3), "personally identifiable information"  
6 includes information which identifies a person as having requested or obtained specific  
7 video materials or services from a video tape service provider." Defendant knowingly  
8 disclosed Plaintiffs' and the Meta Class members' Private Viewing Information to Meta  
9 in the manner alleged herein. The Private Viewing Information that Defendant  
10 transmitted to Meta constitutes "personally identifiable information" as defined in 18  
11 U.S.C. § 2710(a)(3) because the transmitted information identified Plaintiffs and each  
12 Meta Class member to Meta as an individual who purchased a subscription to video  
13 content from Defendant's website.  
14

15 81. Defendant never obtained informed, written consent from Plaintiffs or any  
16 Meta Class member to disclose their Private Viewing Information to Meta or any other  
17 third party. More specifically, Defendant never obtained from Plaintiffs or any Meta  
18 Class member's informed, written consent in a form distinct and separate from any form  
19 setting forth other legal or financial obligations of the consumer; Defendant never  
20 obtained from Plaintiffs or any Meta Class member's informed, written consent that, at  
21 the election of the consumer, was given at the time the disclosure is sought or was given  
22 in advance for a set period of time, not to exceed two years or until consent is withdrawn  
23 by the consumer, whichever is sooner; and Defendant never provided an opportunity, in  
24 a clear and conspicuous manner, for Plaintiffs or any Meta Class member to withdraw  
25 consent on a case-by-case basis or to withdraw consent from ongoing disclosures, at the  
26  
27  
28

consumer's election. *See* 18 U.S.C. § 2710(b)(2).

82. Defendant knowingly disclosed such information to Meta because Defendant intentionally installed and programmed the Meta Pixel code on its website, knowing that such code would transmit to Meta the subscription purchased by its consumers and the purchasers' unique identifiers (including FIDs).

83. By disclosing Plaintiffs' and Meta Class members' Private Viewing Information, Defendant violated their statutorily protected right to privacy in the video services they requested or obtained from Defendant. 18 U.S.C. § 2710(c).

84. As a result of these violations, Defendant is liable to Plaintiffs and Meta Class members for damages and other relief as provided by the VPPA.

85. On behalf of themselves and all members of the Meta Class, Plaintiffs seek to enjoin Defendant's future disclosures of its purchasers' Private Viewing Information; liquidated damages in the amount of \$2,500 per violation of the VPPA; reasonable attorneys' fees and costs; and all other preliminary or equitable relief the Court deems appropriate. 18 U.S.C. § 2710(c)(2)(A).

**COUNT TWO**  
**Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710**  
**Google Class**

86. Plaintiffs repeat the allegations from paragraphs (1-74) as if fully set forth herein.

87. Plaintiffs bring this claim individually and on behalf of the Google Class Members against Defendant.

88. The VPPA prohibits a “video tape service provider” from knowingly disclosing “personally identifying information” concerning any “consumer” to a third



1 party without the “informed, written consent (including through an electronic means  
2 using the Internet) of the consumer.” 18 U.S.C. § 2710.

3       89. As defined in 18 U.S.C. § 2710(a)(4), a “video tape service provider” is “any  
4 person, engaged in the business, in or affecting interstate or foreign commerce, of rental,  
5 sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials[.]”  
6 Defendant is a “video tape service provider” as defined in 18 U.S.C. § 2710(a)(4) because  
7 it is engaged in the business of delivering audiovisual materials that are similar to  
8 prerecorded video cassette tapes and those sales affect interstate or foreign commerce.  
9

10       90. As defined in 18 U.S.C. § 2710(a)(1), a “consumer” means any renter,  
11 purchaser, or consumer of goods or services from a video tape service provider.” As  
12 alleged above, Plaintiffs and Google Class members are subscribers to Defendant’s  
13 prerecorded video content service. Thus, Plaintiffs and the Google Class members are  
14 “consumers” as defined in 18 U.S.C. § 2710(a)(1).  
15

16       91. As defined in 18 U.S.C. § 2710(a)(3), “personally identifiable information”  
17 includes information which identifies a person as having requested or obtained specific  
18 video materials or services from a video tape service provider.” Defendant knowingly  
19 disclosed Plaintiffs’ and the Google Class members’ Private Viewing Information to  
20 Google in the manner alleged herein. The Private Viewing Information that Defendant  
21 transmitted to Google constitutes “personally identifiable information” as defined in 18  
22 U.S.C. § 2710(a)(3) because Google is an email service and electronic communication  
23 service provider akin to an ISP that stores IP addresses alongside other user  
24 information (name, email, phone number) and the information transmitted by  
25 Defendant informed Google of (1) Plaintiffs IP addresses that directly link back to their  
26  
27  
28

1 Gmail accounts, (2) other information sufficient to identify Plaintiffs, and each Google  
2 Class member, and (3) the specific video materials requested or obtained from  
3 Defendant's website.

4  
5 92. Defendant never obtained informed, written consent from Plaintiffs or any  
6 Google Class member to disclose their Private Viewing Information to Meta or any other  
7 third party. More specifically, Defendant never obtained from Plaintiffs or any Google  
8 Class member's informed, written consent in a form distinct and separate from any form  
9 setting forth other legal or financial obligations of the consumer. Defendant never  
10 obtained from Plaintiffs or any Google Class member's informed, written consent that,  
11 at the election of the consumer, was given at the time the disclosure is sought or was  
12 given in advance for a set period of time, not to exceed two years or until consent is  
13 withdrawn by the consumer, whichever is sooner; and Defendant never provided an  
14 opportunity, in a clear and conspicuous manner, for Plaintiffs or any Google Class  
15 member to withdraw consent on a case-by-case basis or to withdraw consent from  
16 ongoing disclosures, at the consumer's election. *See* 18 U.S.C. § 2710(b)(2).

17  
18  
19 93. Defendant knowingly disclosed such information to Google because  
20 Defendant intentionally installed and programmed the Google Analytics code on its  
21 website, knowing that such code would transmit to Google or allow Google to  
22 simultaneously collect the specific video titles requested or obtained on Defendant's  
23 website, the user's IP address, and other information sufficient for Google to identify  
24 the particular subscriber.

25  
26 94. By disclosing Plaintiffs' and Google Class members' Private Viewing  
27 Information, Defendant violated their statutorily protected right to privacy in the videos  
28

1 they requested or obtained from Defendant. 18 U.S.C. § 2710(c).

2 95. As a result of these violations, Defendant is liable to Plaintiffs and Google  
3 Class members for damages and other relief as provided by the VPPA.

4 96. On behalf of themselves and all members of the Google Class, Plaintiffs  
5 seek to enjoin Defendant's future disclosures of its purchasers' Private Viewing  
6 Information; liquidated damages in the amount of \$2,500 per violation of the VPPA;  
7 reasonable attorneys' fees and costs; and all other preliminary or equitable relief the  
8 Court deems appropriate. 18 U.S.C. § 2710(c)(2)(A).  
9  
10

### 11 **PRAYER FOR RELIEF**

12 WHEREFORE, Plaintiffs, individually and on behalf of all others similarly  
13 situated, seek a judgment against Defendant Yanka Industries Inc. d/b/a MasterClass.  
14 as follows:  
15

- 16 A. For an order certifying the Classes under Rule 23 of the  
17 Federal Rules of Civil Procedure and naming Plaintiffs as  
18 representatives of the Classes and Plaintiffs' attorneys as  
Class Counsel to represent the Classes;
- 19 B. For an order declaring that Defendant's conduct as described  
20 herein violated the VPPA;
- 21 C. For an order finding in favor of Plaintiffs and the Classes and  
22 against Defendant on all counts asserted herein;
- 23 D. For an award of \$2,500.00 to the Plaintiffs and members of the  
24 Classes, as provided by the VPPA, 18 U.S.C. § 2710(c);
- 25 E. For an order permanently enjoining Defendant from disclosing  
26 the Private Viewing Information of its subscribers to third  
27 parties in violation of the VPPA.
- 28 F. For prejudgment interest on all amounts awarded; and

1  
2 G. For an order awarding punitive damages, reasonable  
3 attorneys' fees, and costs to counsel for Plaintiffs and the  
4 Classes under Rule 23 and 18 U.S.C. § 2710(c).

5  
6 **JURY DEMAND**

7  
8 Plaintiffs demand a trial by jury on all causes of action and issues so triable.

9  
10 Dated: October 24, 2024

11 Respectfully submitted,

12 /s/ Frank S. Hedin

13 **HEDIN LLP**

14 FRANK S. HEDIN

15 535 Mission Street, 14th Floor

16 San Francisco, CA 94105

17 TELEPHONE: (305) 357-2107

18 FACSIMILE: (305) 200-8801

19 [FHEDIN@HEDINLLP.COM](mailto:FHEDIN@HEDINLLP.COM)

20  
21 *Attorney for Plaintiffs and Putative Classes*  
22  
23  
24  
25  
26  
27  
28